REMARKS

Claims 1-77 are pending in the application. Claims 1-23, 25-28, 30, 33, 36, 44, 47-51, 53-56, 58, 61, 64, 72, 75, and 77 are currently amended.

Each of claims 1, 20, and 48 have been amended to recite a concept of decrypting the ballot or structure for ballot decryption. For example, claim 1 now recites "program instructions operable to convert the computer readable form from an encrypted to a decrypted state such that in the decrypted state the computer readable form includes." This concept finds support, for example, on page 33 at lines 15-18, pages 36-37 in the carryover paragraph, and other places in the specification. Claim 20 has been similarly amended to recite "decrypting the ballot viewer object to produce a decrypted ballot viewer object." Claim 48 has been similarly amended to recite "means for decrypting the encrypted ballot viewer object to provide a decrypted ballot viewer object." The remaining claims have been amended to correct for antecedents arising form these amendments. Claim 2 has been amended to recite specific types of voter authentication information, such as mother's maiden name, etc., as recited on page 6 at lines 1-10, page 55 at line 5 and page 46 at lines 12-13 of the specification. Claim 75 has been amended to correct a misspelling of the word "form."

The amendments to insert a concept of decrypting the ballot object or computer readable form show that the process and code for authenticating the voter is distinct from and in addition to the separate authentication that is also required. This concept is implemented on the voter's personal computer, as opposed to being implemented at a different level on an authentication server before the encrypted ballot is transmitted to the voter.

Claims 1-76 are provisionally rejected under 35 U.S.C §101 for statutory double patenting over copending application serial number 09/753,769. The '769 application is no longer pending—a Notice of Abandonment is dated October 21, 2003. Therefore, we respectfully request withdrawal of the provisional rejection.

Claim 6 stands rejected under 35 U.S.C. §112 second paragraph for indefiniteness. The Office asserts that the term "hash" has an accepted meaning of, "a cryptographic term for a small mathematical summary or digest of an original clear-text data file or message." The Office finds

this is contradictory to the term as used by Applicants, namely, to break up storage locations to position them in different locations." The Office does not cite a reference. Both Applicants' definition and that applied by the Office are consistent with use of the word "hash." Applicants rely upon the attached IEEE definitions including those for "hash," "hashing," and "hash value." Hashing is a technique for arranging a set of items. The items are stored according to their hash value or hash address by application of a hash function to a hash key. To clarify the meaning of hashing, Applicants provide one example in addition to the IEEE Dictionary, namely, pages 540 to 546 from Schildt, C: The Complete Reference, Osborne McGraw Hill, 773 pp (1987) (a discussion of hashing in context of logical and physical locations). "Hashed" as used in claim 6 is sufficiently definite and does comport with the ordinary meaning established in the art. In fact, it is a term of art as recognized by the examiner. In hashing, there is a hash function, such as a lookup table or mathematical algorithm, and this is used to identify data storage locations where a body of information may be broken up into discrete components and stored in locations that are identified by the hash function. There is no dispute here because we are talking about the same thing. Therefore, we request withdrawal of the §112 rejection of claim 6.

The Office objects to the amendment filed 9/22/03 because the amendment is said to incorporate new matter by reciting that the interface for batch control processing includes program logic for creating and delivering electronic messages to prospective voters, the electronic messages configured to facilitate a download of an electronic ballot for use by an individual voter. The Office does not specify a particular claim; however, this is the subject matter of claim 77, which has not been considered by the Office. We assume that claim 77 is meant, and request clarification from the Office that claim 77 is intended. We traverse the requirement to cancel the subject matter because it does have support, for example, as provided in these excerpts from the published application, and in other places of the Specification:

> [0077] In yet another aspect of the invention according to its various embodiments, the previously described instrumentalities may be implemented as improvements to existing postal service email servers. In an official postal server authorized by a national government agency for the transmission of electronic data, the improvements comprise an

interface for batch control processing of electronic ballot information as directed by an election server. . . .

0079] The United States Postal Service (USPS) has developed through interaction with the private sector a secure electronic document transfer service named POSTeCS[2] which may optionally be used to secure the communications channels from election headquarters to the voter and return. The POSTeCS system operates as an electronic mail delivery service and can be used to transfer the ballot to the voter and return the voter's cast ballot to the election . For example, the voter may receive an email that contains a unique URL that is associated with a downloadable form of ballot viewer object 100. The server containing the URL is preferably configured to only transmit the data if a proper SSL link is established between server and the voter's computer. Thus, whenever the user clicks the unique URL link, an SSL session will be established to secure the transmission of the ballot viewer object 100.

[0080] In more general terms, the POSTeCS service allows a vendor to send an email message to a customer. The message points the customer to an electronic download. The customer's actions of receiving the email, opening the email, and downloading the file are tracked by the USPS, which provides information on the status of the transfer to the customer. The download information is encrypted and transmitted securely, for example using SSL, and the downloads are encrypted while they reside on the USPS server. Before the customer is allowed to download the file, the customer may be asked to enter a password. The USPS charges a transactional fee similar to postage for this service. . . . .

[0083] FIG. 6 depicts a general overview of the major operational components relating to the POSTeCS server 600. These components are subject to modification, as described below, to improve operability of the POSTeCS server 600 for purposes of the preferred embodiments of the invention. Any other server or system having similar functionality may replace the POSTeCS server 600. By analogy, the POSTeCS server 600 functions as a normal email server, however, various functions have been added to permit the USPS to charge a transactional fee in transmitting secure email. The POSTeCS server acts as a postman would in carrying and delivering a letter for a fee. The POSTeCS server 600 resides on a server (or servers) 602, which functions as an electronic mail server in support of a plurality of clients, e.g., clients 602, 604, and 606, who wish to send and receive messages. A queuing agent 608, e.g. a conventional message database, may be used to temporarily store message data. Standard messaging protocols are used to transmit and receive messages through the Internet 610 among the respective clients . . .

[0085] The existing POSTeCS system may be modified to implement the concept of replicating electronically the "self-addressed stamped envelope, " which would permit the voter to act as a customer in voting by absentee ballot with a transactional fee through

> simplified batch processes excluding the cumbersome registration and downloading processes. Charges may, for example, be prepaid by the voter at the time of voter registration or directed to a charge card that the voter authorizes for use at the time of registering to vote. . . .
>
> [0088] Once the process control function 704 authorizes the connection with the election headquarters server 208, function 706 entails the transmission of voter emails, which may be coupled with an electronic ballot such as ballot viewer object 100. These emails are preferably but optionally transmitted as a batch job that originates from pre-transmission services at election headquarters.

The foregoing excerpts provide support for claim 77 and refute the new matter objection.

Claims 1-75 are rejected under 35 U.S.C. §103(a) over US 6,081,793 to Challener, US 6,250,548B1 to McClure et al., and in further view of the Symantec AntiVirus Research Center publication which is selectively applied to claims 18, 19, 46, 47, 74 and 75. Challener is said to disclose all aspects of claim 1, except that the display code is used to display the official ballot image to the voter. McClure is used to show that a display code may display an official ballot image. No reason is given why there is a suggestion or motivation to combine these references other than a statement that "it would be obvious" to do so; however, the Office does observe that the Challener '793 system does have a ballot dispensing system (col. 3 at lines 25-26). Thus, it is the Office's position that McClure 548 shows one type of code that may be transmitted using the Challener system. We traverse the rejection for the reasons explained below.

Where there is a separate code for or process of decryption the combination of references does not teach or suggest these features of claim 1:

> wherein the computer readable form does not require voter authentication code is configured to authenticate a voter for voting on a personal computer without requiring a server to assist in authenticating an individual voter while the display code is present on the personal computer.

Where there is a separate code for or process of decryption the combination of references does not teach or suggest these features of claim 20:

> the step of authenticating the voter being performed after the step of downloading the ballot and before the step of transmitting the cast vote record by executing voter authentication code from the ballot viewer object and authenticating the voter without interacting with the server after the step of downloading the ballot viewer object.

Where there is a separate code for or process of decryption the combination of references does not teach or suggest these features of claim 48:

> the means for authenticating the voter being configured for operation sequentially after execution of the means for downloading the ballot and before execution of the means for transmitting the cast vote record,
>
> the means for authenticating the voter including executable authentication code obtained from the ballot viewer object,

This is because the process of authentication being claimed is separate and distinct from decryption where, for example as recited in claim 2, the authentication information includes such voter personal information as mother's maiden name and children's birthdays. What the foregoing features of claims 1, 20, and 48 share in common is the concept of a ballot that does not require server interaction for authentication once the ballot is downloaded, whereas Challener '793 requires this form of authentication to be performed at a different level, namely on the authentication server in process step 389 as show in Fig. 7 of Challener. For convenience, we will refer to this concept in the discussion below as that of a self authenticating ballot. This concept distinguishes Challener '793, which requires the use of three separate authentication servers, each having a public key and a private key for encryption/decryption purposes (col. 3, lines 37-43). It will be appreciated that while Challener '793 has authentication at many levels, there is no provision made for self-sustaining authentication of the voter while the ballot display code is present on the voter's personal computer as is presently claimed. For example, the passage in column 7 at line 38 to column 8 at line 20 of Challener '793 describes a process where, following authentication, the ballot is encrypted and transmitted to the voter's computer. There is no further authentication until the completed ballot arrives back at the journal server..

The process is shown in Fig. 7 where steps 381, 383, 389, and 393 occur on the "Authentication Server" and step 403 occurs on the journal server.

The Office has repeated in substantially verbatim form what was contained in the previous office action including rejections of the remaining claims in the application. Applicant has previously responded to those rejections and hereby incorporates its previous remarks in rebuttal of those rejections. There should be no ultimate issue because the amended independant dependant claims are allowable for reasons explained above. The dependant claims are likewise allowable, at least because they incorporate the limitations of the base claims form which they depend. Even so, the dependant claims have patentable merit of their own for reasons explained in our earlier response.

At the conclusion of the present action, the Office asserts that it has inserted reference to passages by column number and line number for Applicants' convenience. We wish to thank the Office for this courtesy. On the other hand, the office reminds Applicants that other passages in addition to those relied upon by the Office may be relevant and Applicants are encouraged to read the entire references. While the advisory caution is understood, it is also the case that certain passages expressly relied upon by the Office do not teach what the Office holds them to say, and the foregoing remarks note this in specific instances. This is now the second action that Applicants have received with the same unresolved errors, for example, in regard to the use of video memory in claims 9, 19, 47, and 75. It is absolutely untrue that Challener '793 teaches the claimed use of video memory in column 10 at lines 65-67 and column 11 lines 1-5. The 'historical archive' of those passages is entirely different from the concept of using video memory to confirm that what the voter sees on the PC corresponds to the ballot choices the voter has entered. Also, in regard to the claims that recite downloading the ballot object as an email attachment, the Office consistently asserts that a download of this type solves no recognized problem. Applicants have responded that the problem solve is a self-authenticating ballot that does not require server interaction, which would overcome most servers during an election. The Office has failed to recognize this solution and, further, does not provide a reference that teaches

or suggests this solution need in the art. If the Office is improperly relying upon specific passages for what they do not teach, or if the Office needs a reference in support of its position, it is Applicant's duty to point this out and the duty of the Office to respond to those arguments. The Office must make a specific rebuttal properly supported by the art of record if the Office finds those arguments are in error.

Applicant's attorney respectfully solicits a Notice of Allowance for the reasons discussed above. the undersigned attorney invites the examiner to telephone if a conversation could expedite prosecution. If any fee has been inadvertently overlooked, please charge deposit account number 12-0600.

Respectfully submitted:

Date: 5/18/04

Dan Cleveland, Jr., Reg. No. 36.106
LATHROP & GAGE L.C.
4845 Pearl East Circle, Suite 300
Boulder, CO 80301
Tel: 720 931-3012
Fax: 720 931-3001